**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

In re Sealed Docket Sheet Associated With Malware Warrant Issued on July 22, 2013

Civil Action No. _____

**MOTION TO UNSEAL COURT DOCKET SHEET**

For the reasons stated in the accompanying memorandum of law, the American Civil Liberties Union, the American Civil Liberties Union Foundation, the American Civil Liberties Union of Maryland, and the American Civil Liberties Union Foundation of Maryland respectfully move for this Court to unseal any currently sealed docket sheets associated with any search warrants issued by this Court on July 22, 2013 that authorize the surreptitious use of surveillance software (commonly referred to as "malware") to acquire identifying information from private computers.

August 25, 2016

Respectfully submitted,

David Rocah (Bar No. 27315)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Road
Suite 350
Baltimore, MD 21211
Tel: (410) 889-8550
Fax: (410) 366-7838
Email: rocah@aclu-md.org

Brett Max Kaufman (*pro hac vice* to be filed)
Nathan Freed Wessler (*pro hac vice* to be filed)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad St., 18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2654
Email: bkaufman@aclu.org

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| In re Sealed Docket Sheet Associated With Malware Warrant Issued on July 22, 2013 | Civil Action No. _____ |

**MEMORANDUM OF LAW IN SUPPORT OF**
**MOTION TO UNSEAL COURT DOCKET SHEET**

## Table of Contents

## Table of Authorities

**Cases**

**Other Authorities**

## Introduction

The American Civil Liberties Union, the American Civil Liberties Union Foundation, the American Civil Liberties Union of Maryland, and the American Civil Liberties Union Foundation of Maryland (together, the "ACLU") respectfully move this Court to unseal any sealed docket sheets associated with any search warrants issued by this Court on July 22, 2013 that authorize the surreptitious use of surveillance software (referred to by the FBI as a "Network Investigative Technique" or "NIT" and more commonly known as "malware") to acquire identifying information from private computers. A malware warrant issued by this Court on July 22, 2013 is referenced in an affidavit that was filed in support of an application to search the home of a suspect in *United States v. Klein*, No. 13 Mj. 00117, Doc. 1-3, at 16, ¶ 16.c (D. Vt. Nov. 20, 2013) (attached as "Exhibit C"), but no corresponding warrant appears on the public docket sheet for *United States v. Klein* (attached as "Exhibit A"), or (to the knowledge of the ACLU) on any other public docket sheet. Because the public has First Amendment and common-law rights to access them, this Court should unseal any sealed docket sheets with entries for malware warrants (and related materials) issued by the Court on July 22, 2013.

The terms "NIT" and "malware" refer to code delivered surreptitiously to one or more computers that enables the collection of private information about the user(s), including identifying information such as an IP address.[1] Such code is used by hackers to steal passwords and other personal information.[2] Increasingly, the FBI has used malware to pierce the online

[1] An IP address is "a code that identifies a computer network or a particular computer or other device on a network, consisting of four numbers separated by periods." *IP Address*, Dictionary.com, http://www.dictionary.com/browse/ip-address.

[2] The Ninth Circuit Court of Appeals has described malware as software that "works by, for example, compromising a user's privacy, . . . stealing identities, or spontaneously opening

anonymity and surveil the private communications of those it suspects of committing crimes. For example, the FBI has attempted to use malware to determine the identity of those who are suspected of committing bank fraud over the Internet. But malware can be used to ascertain far more than merely a user's identity: "the software has the capacity to search the computer's hard drive, random access memory, and other storage media[ and] to activate the computer's built-in camera." *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013) (order denying government application for warrant authorizing use of malware). Given, moreover, that "law enforcement agencies are placing malware on sites that might have thousands of users," many worry that "investigators may also wind up hacking and identifying the computers of law-abiding people who are seeking to remain anonymous, people who can also include political dissidents and journalists." Ellen Nakashima, *This Is How the Government Is Catching People Who Use Child Porn Sites*, Wash. Post, Jan. 21, 2016, http://wpo.st/_lRh1 (hereinafter "Nakashima Article").

Although the FBI has used malware for approximately fifteen years, the executive branch has never sought explicit legislative authority to use this surveillance technology. Instead, agencies have sought judicial approval for the use of malware on an ad hoc basis by applying for search warrants under Rule 41 of the Federal Rules of Criminal Procedure.[3]

---

Internet links to unwanted websites . . . ." *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1171 (9th Cir. 2009).

[3] *See generally* Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, And Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 Yale J.L. & Tech. 134, 164 (2013) (describing a trend in which the "government seeks to accommodate the use of new and powerful surveillance technologies through aggressive interpretation of existing statutory language that neither directly authorizes nor prohibits their use").

The breadth and potency of malware as a law-enforcement tool raises concerns that can only be properly debated if legislators and the general public are aware of instances in which it is being used, the ways in which law enforcement seeks to use it, and the extent of judicial supervision. The sealing of docket sheets with warrants authorizing the use of malware prevents this critical public debate from happening, in violation of the public's right of access. *See Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 572 (1980) ("People in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing."). The ACLU therefore respectfully requests that the Court order the unsealing of any docket sheets relating to the government's application for any malware warrants authorized by the Court on July 22, 2013.

**Jurisdiction**

This Court has jurisdiction over this motion due to its inherent "supervisory power over its own records and files." *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 598 (1978).

**Background**

I. The government's use of malware to hack into private computers

The FBI's use of digital spying technology dates back to at least as early as 1999, when a court authorized investigators to install a covert keystroke-logging device on a suspect's computer. Kevin Poulsen, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, Wired, July 18, 2007, http://www.wired.com/2007/07/fbi-spyware (hereinafter "2007 Poulsen Article"). By 2002, the agency had developed a malware tool that could be delivered over the Internet to surveillance targets. *See* Nat Hentoff, *The FBI's Magic Lantern*, Village Voice, May 28, 2002, http://www.villagevoice.com/news/the-fbis-magic-lantern-6413591. But it was not until 2007 that an actual use of malware by the FBI was publicly revealed; the case involved a

teenager who had made bomb threats to his high school. 2007 Poulsen Article. The malware that infected the suspect's computer was used to determine the computer's IP address, log its browsing behavior, and register the IP address of every computer to which it connected.[4] *Id.*

In April 2013, the FBI applied for a warrant authorizing the use of malware targeting a computer belonging to individuals suspected of committing bank fraud and identity theft. *See In re Warrant*, 958 F. Supp. 2d at 755. The malware sought to be deployed could collect massive amounts of information from the targeted computer, such as browsing history, saved passwords, and email and chat communications. *Id* at 755–56. The FBI also intended to use the targeted computer's built-in camera to take surreptitious photos of the individuals who used it. *Id.* at 759–61; *see also* Craig Timberg & Ellen Nakashima, *FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, Wash. Post, Dec. 6, 2013, http://wpo.st/FzRh1(hereinafter "Timberg & Nakashima Article") (noting that, according to former FBI official, the agency had "been able to covertly activate a computer's camera—without triggering the light that lets users know it is recording—for several years"). In a public order, a federal magistrate judge denied the application, finding that the search would violate both Rule 41(b) of the Federal Rules of Criminal Procedure and the Fourth Amendment. *In re Warrant*, 958 F. Supp. 2d at 756–61.

Although the exact number is unclear, the FBI has since deployed malware of differing capabilities in numerous cases. *See* Timberg & Nakashima Article. Marcus Thomas, former assistant director of the FBI's Operational Technology Division, which contains the FBI unit

[4] Importantly, the public appears to have learned of its deployment from an FBI affidavit filed in support of a search warrant application. *See* Gregg Keizer, *FBI Planted Spyware on Teen's PC to Trace Bomb Threats*, Computerworld, July 19, 2007, http://www.computerworld.com/article/2542586/data-privacy/fbi-planted-spyware-on-teen-s-pc-to-trace-bomb-threats.html.

responsible for the agency's use of malware, has stated that the FBI's malware technology continues to advance and that law enforcement agencies are realizing "that they're going to have to use these types of tools more and more." *Id.*

In addition to the tailored use of malware against individual targets, the FBI has, since 2012, engaged in a number mass-hacking operations targeting thousands of individuals by delivering malware to every computer that visits a particular website under the FBI's control. David Bisson, *FBI Used Metasploit Hacking Tool in 'Operation Torpedo,'* Tripwire, Dec. 16, 2014, http://tripwire.me/29efAEC; Joseph Cox, *The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers*, Motherboard, Jan. 5, 2016, http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers. These controversial hacking operations have been criticized by Members of Congress from both parties, *see, e.g.*, Sen. Ron Wyden, Rule 41 Remarks at the Open Tech. Inst., June 30, 2016, *available at* https://www.wyden.senate.gov/news/press-releases/wyden-untested-government-mass-hacking-techniques-threaten-digital-security-critical-infrastructure, and numerous federal courts to have considered the legality of the mass hacking warrants have ruled that such warrants violate Rule 41 of the Federal Rules of Criminal Procedure. *See, e.g., United States v. Levin*, -- F. Supp. 3d --, No. 15 Cr. 10271, 2016 WL 2596010 (D. Mass. 2016); *see also United States v. Matish*, -- F. Supp. 3d --, No. 16 Cr. 16, 2016 WL 3545776, at *17 (E.D. Va. 2016) (collecting cases).

II. The government's use of malware pursuant to a warrant issued by this Court

In July 2013, the FBI seized a group of servers that hosted various websites on the "dark web"—a part of the Internet that cannot be accessed using ordinary search engines. Some, but not all, of the content hosted on these servers—known collectively as the "Freedom Hosting

Network"—was child pornography. Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired, Sept. 13, 2013, https://www.wired.com/2013/09/freedom-hosting-fbi (hereinafter "2013 Poulsen Article").

Among the websites and services on the Freedom Hosting Network was an email service known as "TorMail," which was "used by a range of people, from criminals to dissidents and journalists." Nakashima Article. On August 4, 2013, the homepage of TorMail was, without warning, replaced with a "down for maintenance" message. *Id.* A number of technically sophisticated users noticed that when they visited the TorMail homepage, the website attempted to covertly deliver malware to their computers. 2013 Poulsen Article. Security researchers who subsequently analyzed the code determined that it collected identifying information about visitors to the site and then transmitted that information back to a server in Northern Virginia. The FBI later confirmed that it had deployed malware on Freedom Hosting websites after seizing the Freedom Hosting servers. *Id.*; *see also* Nakashima Article.

On November 20, 2013, the FBI applied in the District of Vermont for a warrant to search the home of Grant L. Klein. *See United States v. Klein*, No. 13 Mj. 00117, Doc. 1 (D. Vt. Nov. 20, 2013) (warrant application, attached as "Exhibit B"). The affidavit supporting the warrant application, submitted by FBI Special Agent Jeffrey W. Alford (the "Alford Affidavit"), indicates that Klein was suspected of visiting an unnamed website during the summer of 2013 that hosted images depicting child sexual exploitation. Alford Aff. ¶ 17.

Agents were aware of this website because "data from the computer server hosting [the website had been] obtained" by the FBI, but anonymity-protecting software prevented the FBI from determining the IP addresses of the website's visitors. *Id.* ¶ 16.b. In order to learn the identities of these visitors, the FBI obtained a warrant from this Court on July 22, 2013 that

authorized the deployment of malware on the website to infect its visitors' computers. *Id.* ¶ 16.c. Between July 31 and August 5, 2013, the FBI used this malware to "identify the computer[s], [their] location[s], other information about the computer[s], and the user[s] of the computer[s] accessing" the website. *Id.*

Using this malware, the FBI determined that on August 4, 2013, a computer used by Klein visited the website and accessed child pornography. *Id.* ¶ 17.a–b. Klein was subsequently convicted of one count of possession of child pornography and sentenced to twelve years of imprisonment and ten years of supervised release. *See* FBI, Press Release, *Brattleboro Man Sentenced to Prison for Child Pornography Offense* (Oct. 28, 2014), http://1.usa.gov/28T3Ohq (hereinafter "Klein Press Release").

While the July 22, 2013 warrant authorizing the use of the malware that led the FBI to identify Klein is referenced in paragraph 16 of the Alford Affidavit, the warrant itself has not been entered on the District of Vermont docket sheet associated with the search warrant for Klein's home and it is (as far as the ACLU can tell) not posted on any public docket sheet in this District, where it was issued. The potentially relevant docket may be one of the four sealed cases initiated on July 22, 2013 and assigned to magistrate judges in this District,[5] or it may be some other docket.

As indicated in the Alford Affidavit, the malware deployed against Klein was used to identify numerous individuals who visited a website that hosted child pornography. Alford Aff. ¶ 16.c. Beyond that, the extent of the malware's deployment is unknown. It is unclear, for instance, how many individuals' computers were infected, in which Districts, and what

[5] The case numbers for these docket sheets are: 13-mj-1553, 13-mj-1554, 13-mj-1567, and 13-mj-1749.

information was obtained. Given that the malware deployed against Klein was delivered to Freedom Hosting website visitors between July 31 and August 5, 2013, and that the TorMail malware was delivered on August 4, there is reason to believe that the website Klein visited was part of the Freedom Hosting Network, and that the malware warrant issued by this Court on July 22, 2013 was the source of authority for the deployment of malware not just against Klein, but across Freedom Hosting websites and services—which had thousands of users—including against innocent users of TorMail.

To date, the only publicly accessible warrants authorizing the FBI to engage in bulk hacking have targeted websites that are dedicated to the distribution of child pornography, and, as a result, the government has been able to assert probable cause that everyone visiting the sites is engaged in a crime. The TorMail website, in contrast, was not dedicated to the distribution of child pornography—it was a free, anonymous email service that had many users who were using it to protect their lawful private communications. Nakashima Article. That the FBI engaged in a bulk hacking operation against all visitors to TorMail, which had many lawful, valid uses, raises serious concerns about the appropriateness of bulk hacking, and the extents to which courts should be authorizing and supervising such operations.

The sealing of the docket sheet associated with the July 22, 2013 warrant prevents these concerns from being aired and debated publicly. Indeed, it prevents the public from learning or confirming even the most basic facts about the deployment of malware for law-enforcement purposes: the fact of judicial approval is unconfirmed; any reasoning supporting such approval is inaccessible; even the reasons for precluding public access are themselves inaccessible. The sealing therefore violates the public's rights under the First Amendment and the common law to access information about the activities of the executive branch and the judicial processes that

authorize them. Any sealed docket sheets relating to the malware warrant issued by this Court on July 22, 2013 should therefore be unsealed.

**Standing**

"Members of the public have standing to move to unseal criminal proceedings." *United States v. Ring*, 47 F. Supp. 3d 38, 41 (D.D.C. 2014) (citing *Press-Enter. Co. v. Superior Court*, 478 U.S. 1 (1986) ("*Press-Enterprise II*")); *see also In re Knight Publ'g Co.*, 743 F.2d 231, 234 (4th Cir. 1984) ("[R]epresentatives of the press and general public 'must be given an opportunity to be heard on the question of their exclusion.'" (quoting *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596 (1982)). The ACLU has standing to bring this public-access motion because it has suffered an injury-in-fact that is fairly traceable to the sealed docket sheet associated with the malware warrant issued by this Court on July 22, 2013. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992); *see also N.Y. Civil Liberties Union v. N.Y. City Transit Auth.*, 684 F.3d 286, 294–95 (2d Cir. 2011) (finding civil liberties organization had standing to challenge public's exclusion from Transit Adjudication Bureau hearings); *In re Wash. Post*, 807 F.2d 383, 388 n.4 (4th Cir. 1986) (finding newspaper had standing to move to unseal plea hearing transcripts because "it ha[d] suffered an injury that [wa]s likely to be redressed by a favorable decision" (alteration and quotation marks omitted)).

**Argument**

"The right of public access to documents or materials filed in a district court derives from two independent sources: the common law and the First Amendment." *Va. Dep't of State Police v. Wash. Post*, 386 F.3d 567, 575 (4th Cir. 2004). A First Amendment right to access judicial records attaches when the "experience and logic" test is satisfied—that is, when a record has historically been available to the public and when "public access plays a significant positive role

in the functioning of the particular process." *Press-Enterprise II*, 478 U.S. at 8–9. When the right attaches, it "may be overcome only by an overriding interest based on findings that closure is essential to preserve higher values and is narrowly tailored to serve that interest." *Id.* at 9.

The common-law right of access "is rooted in many of the same principles that form the basis of the First Amendment right, including the need for accountability of the otherwise independent judiciary, the need of the public to have confidence in the effective administration of justice, and the need for civic debate and behavior to be informed." *United States v. Sonin*, -- F. Supp. 3d --, No. 15 Cr. 116, 2016 WL 908650, at *2 (E.D. Wis. 2016). It attaches to *all* judicial records, and establishes a presumption of access that can be overcome only "if countervailing interests heavily outweigh the public interests in access." *Rushford v. New Yorker Magazine, Inc.*, 846 F.2d 249, 253 (4th Cir. 1988).

"Regardless of whether the right of access arises from the First Amendment or the common law, it may be abrogated only in unusual circumstances." *Wash. Post*, 386 F.3d at 576 (quotation marks omitted). The sealing of an entire docket sheet—the openness of which is a prerequisite to accessing any of the underlying docket entries, *Hartford Courant Co. v. Pellegrino*, 380 F.3d 83, 93 (2d Cir. 2004)—is "particularly troubling," and therefore viewed with special skepticism, *Stone v. Univ. of Md. Med. Sys. Corp.*, 855 F.2d 178, 182 (4th Cir. 1988). Accordingly, the Fourth Circuit has already recognized a right of access to criminal docket sheets,[6] *In re State-Record Co.*, 917 F.2d 129, 129 (4th Cir. 1990) (per curiam), bringing the docket-sheet unsealing sought here squarely within Circuit precedent, *see, e.g.*, *In re Search Warrant for Secretarial Area Outside Office of Gunn*, 855 F.2d 569, 573 (8th Cir. 1988) ("[A] search warrant is certainly an integral part of a criminal prosecution.").

[6] And civil docket sheets. *See Doe v. Pub. Citizen*, 749 F.3d 246, 268–69 (4th Cir. 2014).

As explained more fully below, there is no basis for keeping the docket sheet associated with the malware warrant issued by this Court on July 22, 2013 sealed, and the ACLU's motion should therefore be granted.

## I. The First Amendment requires unsealing the docket sheet listing the malware warrant issued in this District.

### A. A constitutional right of access applies to the docket sheet listing the malware search warrant.

To determine whether the First Amendment right of access attaches, a district court must ask first, "whether the place and process have historically been open to the press and general public," and second, "whether public access plays a significant positive role in the functioning of the particular process in question." *Press–Enterprise II*, 478 U.S. at 8–10; *see Balt. Sun Co. v. Goetz*, 886 F.2d 60, 64 (4th Cir. 1989).

#### 1. There is a "centuries-long" tradition of access to docket sheets.

The "experience" prong of the test is easily satisfied. This country has a "centuries-long history of public access to dockets." *United States v. Mendoza*, 698 F.3d 1303, 1304 (10th Cir. 2012). "Since the first years of the Republic, state statutes have mandated that clerks maintain records of judicial proceedings in the form of docket books, which were presumed open either by common law or in accordance with particular legislation." *Pellegrino*, 380 F.3d at 94. Courts, too, have repeatedly affirmed the public's right to access dockets for a variety of proceedings, civil and criminal. *See Doe v. Pub. Citizen*, 749 F.3d 246, 268–69 (4th Cir. 2014) (civil); *United States v. Ochoa-Vasquez*, 428 F.3d 1015, 1029-30 (11th Cir. 2005) (criminal); *Pellegrino*, 380 F.3d at 96 (civil); *United States v. Valenti*, 987 F.2d 708, 715 (11th Cir. 1993) (criminal); *In re State-Record Co.*, 917 F.2d at 129 (criminal); *Webster Groves Sch. Dist. v. Pulitzer Publ'g Co.*, 898 F.2d 1371, 1377 (8th Cir. 1990) (civil); *Bernstein v. Bernstein*, No. 14 Civ. 6867, 2016 WL

1071107, at *1 (S.D.N.Y. Mar. 18, 2016) (civil); *In re Application to Unseal 98 Cr. 1101 (ILG)*, 891 F. Supp. 2d 296, 298 (E.D.N.Y. 2012) (criminal); *cf. United States v. Index Newspapers, LLC*, 766 F.3d 1072, 1085 (9th Cir. 2014) (contempt).

To be sure, "the process of issuing search warrants has traditionally not been conducted in an open fashion." *Gunn*, 855 F.2d at 573; *see Goetz*, 886 F.2d at 64. But even "search warrant applications and receipts are routinely filed with the clerk of court without seal." *Gunn*, 855 F.2d at 573. And, of course, the historical accessibility of these docket *entries* has depended on the docket *sheets* themselves being publicly accessible. *See id.* at 575 (recognizing First Amendment right to access search warrant docket sheet under history and logic test); *cf. Globe Newspaper Co. v. Fenton*, 819 F. Supp. 89 (D. Mass. 1993) (same as to index of criminal cases). Thus, even when finding sufficient ground to seal a warrant itself, the Fourth Circuit has emphasized that search warrant docket sheets and as many filings on them as possible should nevertheless remain publicly available. *Goetz*, 886 F.2d at 65.[7]

**2. Logic demands keeping docket sheets open.**

"Logic supports this judgment of history." *Pellegrino*, 380 F.3d at 95. Docket sheets are not merely judicial records—they "provide a kind of index to judicial proceedings and documents," without which "the ability of the public and press to attend civil and criminal cases would be merely theoretical." *Id.* at 93. By the same token, the ability of the public to exercise its

[7] The ACLU is aware of only one occasion on which a right of access to a search-warrant docket sheet was found to be lacking. *See In re Search of Fair Fin.*, 692 F.3d 424 (6th Cir. 2012). The Sixth Circuit found no right of access to "documents filed in search warrant proceedings," and summarily extended this conclusion to the docket sheet itself. *Id.* at 433. The court assumed that docket sheets could be sealed because "docket entries are often detailed and could reveal . . . sensitive information," without assessing history or logic, *id.*, both of which, as explained here, favor openness. It also ignored the tailoring requirement, which favors redactions over wholesale sealing as the proper approach to sensitive information. *See infra* Part I.B.

right to access any individual entries on a docket sheet is foreclosed when the entire docket sheet is sealed. *See Pub. Citizen*, 749 F.3d at 268 ("Our skepticism toward wholesale sealing of docket sheets [i]s grounded in the commonsensical observation that most of the information contained on a docket sheet is material that is presumptively open to public inspection."); *Pellegrino*, 380 F.3d at 94 ("Sealed docket sheets would also frustrate the ability of the press and the public to inspect those documents, such as transcripts, that we have held presumptively open."). Sealing docket sheets also "thwart[s] appellate or collateral review of the underlying sealing decisions. Without open docket sheets, a reviewing court cannot ascertain whether judicial sealing orders exist." *Id.* This is a particularly salient problem in the Fourth Circuit, where procedures governing judicial sealing orders are constitutionally compelled: a district court must provide notice to the public of the request to seal and an opportunity for the public to challenge the request; consider less-drastic alternatives to sealing; and state any reasons for sealing, supported by specific factual findings, on the record. *Stone*, 855 F.2d at 181; *see also United States v. Mohamed*, No. 13 Cr. 120, 2015 WL 224408, at *2 (E.D. Va. Jan. 14, 2015) (observing that these procedures are compelled by due process). When the docket sheet itself is sealed, there is no way to enforce these procedural rights.

The significance of the right of access is, moreover, at its "apex" where, as here, the underlying action implicates "not only functions of the courts but also the positions that its elected officials and government agencies take in litigation." *Pub. Citizen*, 749 F.3d at 271. "[I]n such circumstances, the public's right to know what the executive branch is about coalesces with the concomitant right of the citizenry to appraise the judicial branch." *FTC v. Standard Fin. Mgmt. Corp.*, 830 F.2d 404, 410 (1st Cir. 1987). This case involves judicial approval of the executive branch's use of novel technologies that stretch the limits of existing law. It is crucial

for the public to be able to engage in an informed debate about such phenomena. The sealing of the docket sheet containing the malware warrant makes this impossible. Unsealing would, at the very least, confirm the existence of the warrant in question and the circumstances of its having been authorized and sealed. These would be crucial steps in informing an urgent public debate.

* * *

For these reasons, public access to docket sheets in general—and the search warrant docket sheet at issue in this case in particular—is necessary for the proper "functioning of the judicial process and the government as a whole." *Globe Newspaper*, 457 U.S. at 606.

**B. There is no governmental interest that outweighs the public's right of access to the malware-warrant docket sheet, and even if there were, sealing the docket sheet is not a tailored means of accommodating that interest.**

Once the First Amendment right of access attaches, the burden to overcome it "rests on the party seeking to restrict access, and that party must present specific reasons in support of its position." *Wash. Post*, 386 F.3d at 575. Access may only be denied if the party can demonstrate a "compelling governmental interest" in support of closure and prove that closure is "narrowly tailored to serve that interest." *Globe*, 457 U.S. at 606–07.

There is, to be sure, a legitimate governmental interest in protecting the integrity of an ongoing investigation. As the Fourth Circuit has recognized, however, "it is not enough simply to assert this general principle without providing specific underlying reasons for the district court to understand how the integrity of the investigation reasonably could be affected by the release of [the] information [sought]." *Wash. Post*, 386 F.3d at 579. "Whether this general interest is applicable in a given case will depend on the specific facts and circumstances presented in support of the effort to restrict public access." *Id.*

The malware warrant in question here was issued by this Court in mid-2013, and by the end of 2014 the sole prosecution known to the ACLU to have resulted from it had already been resolved. *See* Klein Press Release. The existence of the malware operation, moreover, has been officially acknowledged by the FBI. 2013 Pouslen Article. Thus, "the genie is out of the bottle" with respect to information the government may have once had a legitimate interest in protecting. *In re Application to Unseal 98 CR. 1101 (JLG),* 891 F. Supp. 2d 296, 300 (E.D.N.Y. 2012). What remains secret, however, is the very "index" to the proceedings that authorized the deployment of malware. *Pellegrino*, 380 F.3d at 91. Perversely, then, the public is aware of the investigation's existence, and experts have even been able to analyze the malware used by the government, but the most basic details regarding the circumstances under which this operation was judicially authorized remain hidden. The public has a vital interest in knowing this information, which would greatly contribute to the ongoing public debate about the use of malware by law enforcement, and the government has no legitimate interest in keeping it secret.

There is, moreover, an obvious narrower alternative to the wholesale sealing of a docket sheet: the sealing of individual docket entries or, more likely, the redaction of sensitive information from those entries. "[C]areful redaction is clearly a less restrictive means of advancing the state interest." *United States v. Martin*, 684 F. Supp. 341, 343 (D. Mass. 1988) (alteration omitted). As the Fourth Circuit has recognized, "it would be an unusual case in which alternatives [to wholesale sealing] could not be used to preserve public access to at least a portion of the record." *Stone*, 855 F.2d at 182. Accordingly, requests to seal entire docket sheets are routinely rejected as overbroad. *See In re State-Record Co.*, 917 F.2d at 129; *Gunn*, 855 F.2d at 575. That same result should obtain here.

There is, then, no sufficient government interest in keeping the docket sheet itself secret; indeed, until the docket sheet is unsealed, it cannot even be determined whether any individual docket entries should remain sealed. Sealing the docket sheet is an overbroad approach to addressing an undemonstrated interest, and it therefore violates the public's First Amendment right of access.

## II. The common law also requires unsealing the malware docket sheet.

The common-law right of access attaches to "*all* 'judicial records and documents'"—thus obviating the need to apply the "history and logic" test—and can only be "rebutted if countervailing interests heavily outweigh the public interests in access." *Wash. Post*, 386 F.3d at 575 (emphasis added). The common-law presumption of access is particularly strong when the entire record of a case is sealed. *See Oliner v. Kontrabecki*, 745 F.3d 1024, 1025–26 (9th Cir. 2014); *Perez-Guerrero v. U.S. Atty. Gen.*, 717 F.3d 1224, 1235 (11th Cir. 2013). Factors to assess in determining whether the common-law presumption has been overcome include "whether the records are sought for improper purposes, such as promoting public scandals or unfairly gaining a business advantage; whether release would enhance the public's understanding of an important historical event; and whether the public has already had access to the information contained in the records." *Wash. Post*, 386 F.3d at 575.

For reasons similar to those explained above, the sealing of the search warrant docket sheet also violated the public's common-law right of access. Much of the information protected by the seal—such as the existence of the malware operation, its timing, and the websites targeted—"has already become a matter of public knowledge," which obviates the justification for keeping it secret. *Id.* at 579. At the same time, there is important information on the docket sheet about the judicial authorization of the investigation that would "enhance the public's

understanding of an important historical event," *id.* at 575, such as the existence of any judicial reasoning behind the approval and any justifications offered by the government for the wholesale sealing. (The absence of this information on the docket sheet would be equally valuable to know.) Indeed, the mere fact of judicial approval has never been confirmed. The government could hardly claim an interest in preserving the secrecy of this fact. The public, on the other hand, has a strong interest in confirming that there was judicial approval of this extraordinary investigative technique—something it cannot do without access to the docket sheet in question.

It is, in short, difficult to "understand how the docket entry sheet could be prejudicial" in any way to the government's interests, but easy, on the other hand, to see how disclosure would benefit the public. *In re State-Record Co.*, 917 F.2d at 129. Like the First Amendment, the common law therefore requires unsealing.

**Conclusion**

For the reasons explained above, the ACLU respectfully requests that this Court unseal any sealed docket sheets associated with any malware warrants issued by this Court on July 22, 2013.

August 25, 2016

Respectfully submitted,

David Rocah (Bar No. 27315)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Road
Suite 350
Baltimore, MD 21211
Tel: (410) 889-8550
Fax: (410) 366-7838
Email: rocah@aclu-md.org

Brett Max Kaufman (*pro hac vice* to be filed)
Nathan Freed Wessler (*pro hac vice* to be filed)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad St., 18th Floor
New York, NY 10004
Tel: (212) 549-2500
Fax: (212) 549-2654
Email: bkaufman@aclu.org

**Certificate of Service**

Information regarding the Assistant United States Attorney responsible for the potentially sealed docket sheets is unavailable. However, I hereby certify that on August 25, 2016, I filed the foregoing motion and memorandum of law with the Clerk of the Court and served the same upon the following individual via First Class U.S. Mail:

Rod J. Rosenstein
United States Attorney for the
District of Maryland
36 S. Charles Street, 4th Floor
Baltimore, MD 21201

August 25, 2016

David Rocah (Bar No. 27315)